U.S. General Services Administration (GSA)

GSA Order: GSA Internal Data Sharing Policy

CIO 2109.1A
GSA IT
AskCDO@gsa.gov

Purpose:

This order articulates the policy that organizations within the General Services Administration (GSA) must follow when internally sharing or accessing data.

Background:

This order is intended to establish the governance required to enable the sharing of data assets within GSA.

Applicability:

This Order applies to:

1. All GSA employees, contractors, and subcontractors that may have a need to access or share data, as well as system-to-system data exchanges;
2. The Office of Inspector General (OIG) only to the extent that the OIG determines the order is consistent with the OIG's independent authority under the IG Act and does; not conflict with other OIG policies or the OIG mission; and;
3. The Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines the order is consistent with the CBCA's independent authority under the Contract Disputes Act and does not conflict with other CBCA policies or the CBCA mission.

Cancellation:

This Order does not cancel or supersede any previous Order.

Signature

/S/_____ 2/27/2024_____

David Shive
Chief Information Officer
Office of GSA IT

Date

Table of Contents

1. Purpose

The purpose of this order is to establish the General Services Administration (GSA) as a "share first" organization for data and information. GSA promotes the openness and sharing of data to the greatest extent possible within the agency to promote evidence-based decision making. This order articulates the policy that organizations within the GSA must follow when internally sharing or accessing data. This policy was developed in collaboration with relevant stakeholders to ensure timely access to reliable and high-quality data, while safeguarding GSA's information, privacy, security, and confidentiality.

2. Key Objectives

The objectives of this Internal Data Sharing Policy are to (a) formally establish policy for GSA staff to share data within the agency, (b) create a comprehensive framework that guarantees the responsible handling of data, taking into account all relevant legal, ethical, and security considerations, and (c) improve the level of collaboration between GSA organizations. As changes to the GSA data landscape and capabilities are made, this policy will be reviewed and updated accordingly.

3. Background

GSA organizations rely on the data from various parts of the agency to make informed, evidence-based decisions to achieve its mission. However, data-sharing policies and agreements are currently independently managed directly between parties, leading to a patchwork of non-standard agreements. To improve the utility of its data assets, GSA must establish an agency-wide data sharing policy to enable the free exchange of data across the agency. This policy establishes the governance necessary to internally share data assets efficiently, safely, and responsibly.

4. Related Policies and Procedures

In developing the Internal Data Sharing Policy, GSA reviewed the other policies impacting how agency data is secured and shared. The section below highlights the most relevant policies. Additional policies are referenced in Appendix A.

A. GSA Information and Data Quality Handbook[1]

Provides a framework for consistent information and data management. This handbook helps GSA leverage data for its business purposes and

[1] GSA Information and Data Quality Handbook

achieve the agency's mission.

B. GSA Information Technology Security Policy[2]

Serves to enable GSA to meet its mission and business objectives while protecting IT systems and confidential data. This IT Security Policy establishes security and privacy controls required to comply with Federal laws and regulations (including CISA Cybersecurity Directives) and facilitates adequate protection of GSA IT resources.

C. GSA Records Management Program[3]

Incorporates, by reference, the GSA Records Management Program Website[4] as the official employee reference vehicle for GSA's records management program, policy, and procedures. This program provides additional direction on implementing recordkeeping requirements and assigns responsibilities.

D. Controlled Unclassified Information (CUI) Policy[5]

Establishes a framework and policy for CUI within the GSA. CUI refers to unclassified information that must be safeguarded and controlled for dissemination in compliance with relevant laws, regulations, or Government-wide policies. The CUI Registry[6], maintained by the National Archives and Records Administration (NARA), lists all such information.

E. IT Security Procedural Guide: Managing Information Exchange Agreements, CIO-IT Security 24-125[7]

Identifies the types of information exchange agreements required for GSA systems and the process for establishing the agreements and obtaining approval.

5. Definitions

A. **Data** - Data is a valuable organizational asset encompassing all information that is collected, stored, processed, and utilized by the agency to support its business activities and decision-making processes. Data includes, but is not limited to, raw data or measurement data, statistics, records,

---

[2] GSA Information Technology (IT) Security Policy
[3] GSA Records Management Program
[4] GSA Records Management Program Website
[5] Controlled Unclassified Information (CUI) Policy
[6] NARA.Controlled unclassified information (CUI)
[7] IT Security Procedural Guide: Managing Information Exchange Agreements, CIO-IT Security 24-125

documents, files, and any other form of information that is essential for the organizations' operations, analytics, compliance, and strategic planning. Data may be structured, semi-structured, or unstructured, and includes all associative metadata and paradata[8], as well as any synthetic data products that are derived from data holdings.

B. **Internal Data Sharing**[9] - The process of securely and reliably making the same data available to multiple users, applications, or organizations within GSA while ensuring the integrity of the data. This practice enables authorized users to access data while adhering to applicable data governance standards. All data-sharing initiatives within GSA SHALL comply with agency-wide statutory, regulatory, and security mandates.

C. **Data Asset**[10] - A collection of data elements or datasets that can be grouped together. Each SSO determines the data assets necessary to support their respective mission or business functions. Data assets can represent a database of multiple distinct or single-entity classes.

D. **Dataset**[11] - A dataset is a structured collection of data. The simplest form of a dataset is data elements arranged in a table format. However, a dataset can also present information in various non-tabular formats such as an Extended Mark-Up Language (XML) file, a geospatial data file, or an image file. It is important to note that the dataset follows the required confidentiality, integrity, and availability controls for GSA, adhering to the National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidance.

E. **Personally Identifiable Information (PII)**[12] - PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. GSA protects PII through various methods including security technologies and access controls.

F. **Disclosure Avoidance Measures** - Refers to the efforts to reduce the risk of disclosing CUI in data that is released to the public. Data disclosure avoidance plans are mandatory for GSA's data releases. Properly planning for and implementing disclosure avoidance methodologies is important because each data release affects the risk of disclosure for all related past

[8] US Census Bureau - Research Matters - Paradata
[9] GSA Information and Data Quality Handbook
[10] Enterprise Data Inventories
[11] GSA Information and Data Quality Handbook
[12] Personally Identifiable Information (PII)

and future releases.

6. Responsibilities

Identification of Responsible Departments and Personnel - The following people and groups are involved in implementing this policy:

A. **Chief Information Officer (CIO)** - Responsible for providing guidance and support to the Administrator and other senior management personnel in acquiring and managing information technology and resources in accordance with the policies and procedures outlined in Subtitle III of Title 40, Chapter 113 - Agency Chief Information Officer[13], and the priorities established by the Administrator. Additionally, the CIO manages and oversees the internal information technology program as required by subtitle II Chapter 35 of Title 44 - Coordination of the Federal Information Security[14], and provides technical support and program assistance for shared information processing and data communications used by GSA services and staff offices. The CIO also determines the costs for such support and services.

B. **Chief Data Officer (CDO)**[15] - Manages data assets, coordinates with officials, and ensures that agency data conforms to data management best practices. The CDO also collaborates with the CIO to improve the infrastructure and reduce barriers that inhibit data asset accessibility. The CDO oversees the implementation, compliance, and management of GSA's CUI program and manages the agency's privacy program.The CDO has been delegated as the Senior Agency Official for Privacy (SAOP) for GSA.

C. **Chief Privacy Officer (CPO)** - Responsible for overseeing GSA's Privacy Program[16] whose mission is to preserve and enhance privacy protections for all individuals whose personal information is handled by GSA and to encourage transparency of GSA operations involving PII.

D. **Data and Evidence Governance Board (DEGB) Leads**[17] - Responsible for leading their organization's DEGBs and representing the data management needs of their organization. They ensure that the data priorities of their organization align with GSA's mission and the Federal Data Strategy (FDS)[18]

---

[13] Subtitle III of Title 40, Chapter 113 - Agency Chief Information Officer
[14] Chapter 35 of Title 44 - Coordination of the Federal Information Security, 3554 Federal Agency responsibilities
[15] 4.3 Chief Data Officer Key Stakeholders
[16] GSA Privacy Program
[17] DEGB Roles and Responsibilities
[18] Federal Data Strategy 2021

. The DEGB Leads identify the data assets required for decision-making and ensure all data have assigned Data Stewards. They also work towards improving the quality and trust of data in accordance with the GSA Data Quality Guidelines[19], and ensure that GSA organizations have appropriate data management roles. The DEGB Lead is responsible for ensuring all of their organization's data assets are categorized.

E. **Data Owner**[20] - Collaborates with the System Owner and Data Steward to guarantee that system access is limited to authorized users who have undergone necessary background investigations and requisite security awareness training programs. The Data Owner consults with the Data Steward on the categorization of data assets and is familiar with internal security and privacy protocols.

F. **Domain Steward** - Serves as a Subject Matter Expert (SME) and custodian for one or more of their organization's data domains and the data assets contained within these domains. A Domain Steward helps other GSA stakeholders better understand, standardize, and use domain data to improve their data-driven decision making processes.

G. **Data Steward**[21] - Serves as a SME and custodian for one or more of their organization's enterprise data assets. A Data Steward helps other GSA stakeholders better understand and use the data assets to improve their data-driven decision making processes. The Data Steward works with System Owners to continually improve agency data. The Data Steward is responsible for categorizing data assets based on the framework set forth in this policy, and adding categorization levels to the GSA Data Inventory and Data Catalog.

H. **System Owner**[22] - Responsible for overseeing the technical environments that store and interact with data. It is the responsibility of a System Owner to consider privacy and security requirements when storing and transmitting data. They work closely with Data Stewards to define data requirements and manage access to the data. System Owners also ensure systems and the data each system processes have necessary security controls in place and are operating as intended.

---

[19] GSA Information and Data Quality Handbook
[20] GSA CIO 2100.1P Section 18
[21] Internal Clearance Process for GSA Data Assets
[22] GSA CIO 2100.1P Section 15

7. Data Categorization Framework

A. **Data Categorization Levels** - All data SHALL be classified as either Public, Unrestricted, Controlled, or Controlled Restricted. Data categorization levels SHALL also apply to formalized data about data products, including its metadata and paradata. Any derived data product or information product SHALL also be categorized, and SHALL inherit the most restrictive categorization of its input data sources unless disclosure avoidance measures were applied. GSA organizations MAY choose to create subsets of larger datasets that SHALL then be categorized separately from the original dataset. Definitions for each of the categorization levels are listed below.

1. **Public** - The data asset SHALL be made publicly available without restriction. Public data is by default not CUI.

2. **Unrestricted** - The data asset SHALL NOT be made publicly available and includes agency operational or business data. Unrestricted data is not CUI.

3. **Controlled** - The data asset SHALL NOT be made publicly available and includes agency operational or business data. Controlled data is CUI Basic. CUI Basic[23] is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not have any specific handling or dissemination requirements. CUI Basic SHALL BE handled according to the uniform set of controls set forth in the Code of Federal Regulations (CFR) and the CUI Registry[24].

4. **Controlled Restricted** - The data asset SHALL NOT be made publicly available and includes agency operational or business data. Controlled Restricted data is CUI Specified. CUI Specified[25] is different from CUI Basic in that the authorizing law, regulation, or Government-wide policy contains specific handling controls. The CUI Registry indicates which authorities include such specific requirements. This categorization level includes PII.

B. **Determination of Data Categorization Levels** - The Data Steward in consultation with the Data Owner and Domain Steward SHALL categorize data assets based on the aforementioned categorization levels. The DEGB

[23] eCFR - Title 32 Section-2002.4
[24] Code of Federal Regulations
[25] eCFR Title 32 Section 2002.4

Leads of each GSA organization SHALL be responsible for ensuring all of their organization's data assets are categorized. Categorization levels SHALL be maintained in the GSA Data Inventory and Data Catalog.

C. **Governance for Data Categorization** - GSA organizations SHALL convene a local governance body to adjudicate any categorization level discrepancies or issues. GSA organizations SHOULD consult with the CUI Program Office in GSA-IT for any questions regarding the categorization of CUI data. Any disagreements between GSA organizations regarding the categorization of data SHOULD be escalated to the DEGB Leads of the data owning organizations, and brought to a DEGB Leads meeting for adjudication.

D. **Data Standard Guidelines and Documentation** - In order to optimize data sharing initiatives, data and associated metadata SHALL be consistently maintained and of good quality. GSA organizations SHALL use the data quality descriptions referenced in the GSA Information and Data Quality Handbook as a guideline. Data SHALL also be in open, standard formats (e.g., JavaScript Object Notation (JSON), XML, Comma-separated values (CSV) etc.) so that GSA can maximize its business value.

E. **System-to-System Data Exchanges** - System-to-system data exchanges SHALL follow the applicable requirements as outlined in CIO-IT Security-24-125 IT Security Procedural Guide: Managing Information Exchange Agreements[26]. All system-to-system data exchanges SHALL include documentation outlining the origin of the data, destination, date of collection and last update, data format, associated protocols, and any additional metadata required.

8. Data Discovery and Access

A. **Data Discovery and Access -** Data assets SHALL be centrally discoverable in one location with associated metadata. GSA organizations SHALL follow the access request process for the applicable data warehouse or system. As a best practice, data SHALL NOT be shared via e-mail exchange. Additionally, to maintain data integrity, data SHALL be shared from a centralized source and should not be copied into multiple environments (platforms, databases, systems, etc.).

B. **Role Based Access and Attributes** - Implementation of role based access within

[26] GSA IT Security Procedural Guide: Managing Information Exchange Agreements CIO-IT Security-24-125

IT systems SHALL comply with this policy. Associated attributes for role based access SHALL be used to further protect data and help to streamline access rather than hinder or be overly restrictive.

C. **Data Access Approvals** - GSA has developed a minimum set of approvals necessary to access data based on the categorization levels referenced in Section 7. Refer to the below information for specific approvals needed by GSA employees and contractors to access data assets based on categorization level.

    1. **Public** - No approval required
    2. **Unrestricted** - No approval required
    3. **Controlled** - Requestor's supervisor approval required
    4. **Controlled Restricted** - Requestor's supervisor and Data Steward approval required

GSA organizations SHALL NOT require any additional approvals for data access other than those cited above (note, however that in some cases separate approvals may be required to access specific tools to view and/or analyze data). The supervisor and Data Steward SHALL adjudicate (approve or disapprove) all data access requests within 2 business days of receiving the request. If approval is not granted within the allotted time period, data access SHALL NOT be granted.

GSA organizations MAY include additional governance around the internal deliberation of data access requests. However, all organizations SHALL still maintain compliance with all aspects of this policy. For example, GSA organizations MAY choose to discuss and adjudicate access requests for Controlled Restricted data at a local governance body before the Data Steward approves or disapproves the request.

For Controlled Restricted data the requestor's supervisor SHALL confirm that the individual requesting access has undergone a successful Tier II background investigation per CIO 2100.1P GSA IT Security Policy[27].

Additionally, for Controlled and Controlled Restricted data, the supervisor SHALL ensure that the individual requesting access has a lawful government

[27] GSA CIO 2100.1P

purpose to access the data. This determination SHALL then also be confirmed by the Data Steward for Controlled Restricted data. NARA defines lawful government purpose as “any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities”. The supervisor and Data Steward SHALL consider this definition of lawful government purpose as the criteria for approving access to Controlled and Controlled Restricted data. Furthermore, only the Data Steward for the authoritative data source is authorized to share the requested data.

D. **Safeguarding Data During the Data Access Process** - All data SHALL be protected during the data access process in accordance with the GSA policies and guidance listed in Appendix A.

E. **Data Access Appeals** - In the event the data access request for Controlled Restricted data is denied by the Data Steward, the requestor’s organization can opt to appeal this decision. Appeals will be brought to a governance body chaired by the Chief Data Officer’s Office. Appeal decisions SHALL be jointly made by principal leaders in the requesting GSA organization and the applicable Data Steward’s organization. In the event a joint decision cannot be reached, the decision for data access SHALL be made by the Administrator’s office.

9. Enterprise Data Solution (EDS)

A. **Enterprise Data Solution** - EDS is an ecosystem for centralized data, reporting, and analytical services for GSA. As part of the EDS, GSA-IT SHALL provide a persistent environment for GSA organizations to leverage when conducting statistical and other analysis on datasets. The EDS SHALL also include a set of governance processes to ensure the appropriate collaboration between the requesting GSA organizations and the Data Stewards (and the Data Stewards' organization) when accessing data from another domain or business unit.

Appendix A : References

1. GSA CIO 1878.3 CHGE 2 - Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
2. GSA CIO 2100.1P - GSA Information Technology (IT) Security Policy
3. GSA CIO 2100.3C - Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities
4. GSA CIO 2180.2 - GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
5. GSA CIO Order 2200.1 - GSA Privacy Act Program
6. GSA CIO 2231.1 - CIO GSA Data Release Policy
7. GSA CIO 9297.2C CHGE 1 - GSA Information Breach Notification Policy
8. GSA CIO-IT Security-24-125 - IT Security Procedural Guide: *Managing Information Exchange Agreements*
9. OMB Memorandum M-13-13 - Open Data Policy - *Managing Information as an Asset*
10. CUI Categories, Authorities, Markings, and Examples GSA is Likely to Use. https://docs.google.com/spreadsheets/d/1y7ynnpiRat_x8vChCmSBStA1vNrX8TBjw_g0UE9X4K4/edit#gid=1529873269
11. ECFR.io. (2023). *E-CFR: Code of Federal Regulations*. https://ecfr.io/
12. National Archives and Records Administration. (n.d.). *Controlled unclassified information (CUI)- CUI Registry*. National Archives and Records Administration. https://www.archives.gov/cui